SANS Institute
InfoSec Reading Room

Federal Intrusion Detection, Cyber Early Warning and the Federal Response

Despite strengthened legislation, such as the Federal Information Security Reform Act (FISMA) and the U.S. Patriot Act, initiatives in favor of a cyber early warning system have yet to find staunch supporters outside of the Executive Branch. This paper evaluates Priority One of the National Strategy to Secure Cyberspace, entitled "Priority 1: A National Cyberspace Security Response System," through a contextual analysis of the evolution of cyber early warning in the United States and an evaluation of the underlying tec...

Federal Intrusion Detection, Cyber Early Warning and the Federal Response

Brian Fuller
Version 1.4b Option 1

1.0 INTRODUCTION/ABSTRACT

The February 2003 release of the *National Strategy to Secure Cyberspace* marks the latest indication from the federal government that the United States is still not ready or willing to develop a centralized cyber early warning system. Despite strengthened legislation, such as the Federal Information Security Reform Act (FISMA) and the U.S. Patriot Act, initiatives in favor of a cyber early warning system have yet to find staunch supporters outside of the Executive Branch. Over the past decade, Congress, private industry, and civil rights watchdog groups have aggressively interrupted numerous efforts by the Executive Branch to establish a centralized cyber early warning system.

This paper evaluates Priority One of the National Strategy to Secure Cyberspace, entitled "Priority 1: A National Cyberspace Security Response System," through a contextual analysis of the evolution of cyber early warning in the United States and an evaluation of the underlying technical model. Without a thorough understanding of its evolution, the casual reviewer of the new Strategy probably would not recognize the remnants of what was a contentious proposal to develop a cyber early warning and monitoring system called the Federal Intrusion Network (FIDNet). The repeated assaults on the debate over a centralized cyber early warning system have all but eliminated the last remnants from the National Plan. This paper critically analyzes the technical model for FIDNet, its genesis within the Presidential Commission on Critical Infrastructure Protection (PCCIP) and its evolution through several attempts at a National Plan to protect the United States' critical infrastructures.

2.0 BACKGROUND

Historically, U.S. Early Warning (EW) systems have been capable of detecting preparations by a potential adversary to undertake military action. Since this predictive capability does not exist for cyber attacks, and given the technical and legal complexities of monitoring so many potential cyber adversaries, at least as a first step, EW may consist of detecting an attack as it begins. It is thus critically important to know if it is possible to detect in real time whether an attack is underway. This is not an easy undertaking.

The vision for, and the importance of, an early warning cyber defense derive its origin from World War II. With the lessons of Pearl Harbor still hauntingly vivid, post World War II U.S. leaders invested heavily in technologies to prevent any future surprise strategic or theater attack against the United States or its allies. The dawning age of nuclear weapons, born by increasingly sophisticated generations of intercontinental bombers, spurred huge U.S. investments to develop EW systems and alert mechanisms, such as the Distant Early Warning (DEW) Line and the North American Air Defense (NORAD) system. As Intercontinental Ballistic Missiles and Submarine-Launched Ballistic Missiles became operational, huge research and development investments were made for

new space, ocean and other surveillance and sensor capabilities. As these investments bore fruit, new national technical means were fully and successfully integrated into existing EW systems.

While this Cold War defense strategy suited the threats the United States were facing at the time, the nature of the enemy has since blurred. With traditional warfare, the identity of the attacker is obvious. Short of open warfare, the process of identification becomes much more difficult. For example, the destruction of Pan Am flight 103 required two years of extensive, globe-spanning investigation by multiple countries before the responsible parties were finally identified. Even after a decade has passed since the destruction of TWA flight 800, the complexities of that tragedy still leave unanswered the question of who or what was responsible.[1] Cyber attacks may be even more difficult to resolve. In the event of isolated or cascading infrastructure failures, it may not be possible to immediately establish the attackers motive. Is the failure the result of software or hardware problems? Complex system interdependencies? Operator error? A virus?

The cyber world has no equivalent of the old EW systems like the DEW Line and NORAD, or their modern equivalents. But the need for their cyber equivalents is increasingly apparent in this evolving age of cyber intrusions, cyber terrorism or even cyber warfare.[2] As the government and private industry move toward development of these cyber EW systems, it is informative to consider the contrast between what one must expect from such future systems and existing EW systems. In the world of physical threats, only countries have the financial, technical, and personnel resources to both mount and sustain modern warfare. The low cost of equipment, the readily available technology and cyber tools, and the otherwise modest resources needed to mount a cyber attack against strategic U.S. infrastructures make the number o potential cyber adversaries much greater.

Current EW systems are remarkably effective, if only in part, because of their capability to detect tangible things. They “see” the mobilization of ships, planes, tanks or troops. They “hear” submarines or a surge in the command and control communications necessary to mobilize and deploy forces to combat. Sensors can detect other tangible manifestations, such as the heat plume of a just-launched ICBM. In contrast, a cyber attack may have no tangible components. Unlike the movement of ships, planes or troops, computers and modems are so ubiquitous that their movement is unremarkable. A cyber attack can involve such a small number of people and sites that there will be no surge in command and control communications. So, with good communications security, there will be no “hearable” warning of a cyber attack. Today, preparation for a cyber attack would probably not be detected by U.S. national intelligence assets, thus reducing or eliminating the EW advantage normally enjoyed by the United States.

Indeed, given the complexities of present systems, and the daily challenges of keeping them in operation, the very last thought might be that a system failure is the result of a cyber attack. Carefully prepared and cleverly done, hours, days or weeks may pass before it is determined that such failures were induced intentionally. The greater the time lag, the more difficult it will be to determine who was responsible. Even more confounding are the challenges of non-destructive cyber intrusions, which may well go undetected. It is thus quite easy to conclude that not only is there no cyber EW system to protect U.S. interests, the ability to detect that an attack is underway is limited, particularly if the attack is non-destructive.

In a cyber attack, the first line of defense might well be infrastructure owners and operators, and the local and State government entities whose personnel are the first responders infrastructure emergencies. Under today's legal authorities, the Federal government might well have a secondary or tertiary role in the actual response to a cyber attack. Thus, any cyber EW system that does not fully involve owners/operators and local and State governments is an inadequate system. Moreover, because the range of potential adversaries is so broad, the traditional method of monitoring known adversaries may prove too impracticable. Indeed, such a broad surveillance mandate would likely be unacceptable, particularly as it pertains to domestic monitoring. Thus, the real solution may be EW processes that monitor critical system activity rather than an ever-expanding list of groups or individuals. The range of potential adversaries demands that the U.S. grapple with these issues, both from a technology standpoint and a legal/policy standpoint.

3.0 U.S. GOVERNMENT APPROACH

The U.S. Government has pursued several strategies to address the need for a cyber early warning capability. This section will describe and analyze the original plan articulated in the first national plan to defend cyber space, and proceed by reviewing the recently released National Plan to Secure Cyber Space, specifically the National Cyberspace Security Response System articulated in the plan.

3.1 Original National Plan

In Executive Order 13010 released on July 15, 1996, entitled "Critical Infrastructure Protection," President Clinton stated that certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.[3] As bounded by the Executive Order, threats to these infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats").[4] The Executive Order further stated that, because many of these critical

infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.[5] Toward that end, President Clinton created the Presidential Commission on Critical Infrastructure Protection (PCCIP), and charged it with recommending a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation.[6]

Key sectors of society, including those critical to the national security and the essential functioning of the U.S. economy, are dependent on networked information systems that are vulnerable to cyber attack. These critical infrastructures include communications, transportation, water supply, energy, banking and finance, public health, emergency services, and "continuity of government" functions. The vulnerability of critical infrastructures and the unique risks associated with networked computing have been recognized for some time. But the issue was given new urgency by the report of the PCCIP in October 1997, which highlighted the topic of critical infrastructures and made a series of specific recommendations for their protection. [7]

One of the more intriguing recommendations of the PCCIP was for the establishment of an "early warning and response capability" to protect government and private sector telecommunications networks against cyber-attack.[8] The Commission said that such a capability should include a "means for near real-time monitoring of the telecommunications infrastructure, the ability to recognize and profile system anomalies associated with attacks, and the capability to trace, re-route, and isolate electronic signals that are determined to be associated with an attack.[9]

On May 22, 1998, the President synthesized the findings of the PCCIP and approved Presidential Decision Directive 63, establishing a national critical infrastructure protection policy and a governmental framework to develop and implement infrastructure protection measures.[10] Key organizations created in the directive were a National Infrastructure Protection Center (NIPC), located within the FBI, with operational responsibilities, and a Critical Infrastructure Assurance Office (CIAO), which provided planning and coordination support to a National Coordinator for Security, Infrastructure Protection, and Counter-terrorism (then Richard Clarke), who was located in the National Security Council. A key provision in PDD-63 required the executive branch, through the CIAO and the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, to develop a plan to protect the country's critical infrastructure from attack. Although released a year behind schedule, a dramatically scaled-down national plan was released for public review on January 7, 2000.

3.1.1 FIDNet

A key component of the national plan, one that received considerable attention, is the Federal Intrusion Detection Network or FIDNet. The concept of FIDNet

evolved out of the national security need to protect critical infrastructures from malicious cyber-based attacks.[11] The commissioners working at the PCCIP envisioned a means of monitoring a network for abhorrent or anomalous patterns of behavior that would yield indications of a pending or current attack upon the National Information Infrastructure (NII). The capability would not read the data passing through the network, but rather establish a baseline level of activity the network maintains under normal operating conditions. Once the baseline was established, the monitoring system would then scan the network in real-time to identify patterns of behavior that were anomalous or abhorrent.

The PCCIP, and it members familiar with the telecommunications industry, drew upon this sector's ability to monitor enormous amounts of data and identify anomalous behavior. The key to the telecommunications model, from the government's perspective, was its ability to be somewhat intrusive into the activities of their customers while remaining far enough removed to avoid becoming too invasive so as to raise objections by customers.

The PCCIP members began to explore an intriguing method of profiling, statistical methods, database generation and management, and system scaling that is embedded in toll fraud detection tools.[12] This in-place technology is used to identify anomalies in individual calling patterns. Databases are created consisting of call records which contain information about the date, time, source, destination, and duration of telephone calls. Each international call generates a call record that is stored in a database associated with individual service customers. These databases are called customer call profiles, and there are approximately 12 million active profiles at any time. Tools automatically search profiles for activity and signatures that are indicative of toll fraud activity. Detection of suspected fraud generate alarms, with potential actions including contacting the customer for confirmation and blocking specific call types. Again, a key to this model, procedures and mechanisms are used to protect the privacy of a customer's calling patterns throughout the process.

This toll fraud detection capability was indicative of capabilities currently available to enable the creation and maintenance of individual network activity patterns for large numbers (tens of millions) of users. These profiles evolve over time and can be maintained for years. Deviations from individual profiles of "normal" behavior can be readily detected, new attack signatures identified, and new methods of response developed. Although this particular tool set is used to detect toll fraud in the commercial network, the algorithms used were thought to be adaptable to the profiling of anomalous threats via inappropriate and/or unauthorized network access, and detect the orchestration of an attack distributed across the numerous infrastructures. While applications development still would be required, there was no reason, in principal, why adaptation of these existing methods and tools could not be applied to the data network/Internet areas under the administration of the federal government.[13]

From the toll fraud model, the PCCIP established critical elements that a federal cyber warning system should include to be effective. One of the most crucial elements of a cyber warning system should be the capability to recognize, collect, and profile system anomalies to identify potential threats and/or attacks[14]. This event assessment capability would allow a distinction to be made between indications of "recreational hacking," as opposed to those activities that appear to represent an attack on network operations. It would also facilitate in the systematic identification of suspected and actual intruders through compiling a type of electronic "cyber print" based on algorithms designed to analyze similarities and match behavioral patterns. Fortunately for the Commissioners, the database technology to support this type of capability already was developed and available in commercial form.

The visualization tools to support these sophisticated capabilities must incorporate advanced techniques for displaying very complex, massive data sets. As envisioned for cyber profiling, these tools would display network usage profiles and assist in event detection, threat characterization, and response determination. Although this type of tool set is also commercially available, tailoring to the federal government's specific area of concern would be required.

On a conceptual level, a successful cyber attack warning and response system would require several facets, including:

- A methodology for near real-time monitoring of the telecommunications infrastructure;
- Ability to recognize, collect and profile system anomalies to identify potential threats and/or attacks; and,
- The capability to trace, re-rout, isolate, and destroy electronic signals that are determined to be associated with an attack

Understanding this quandary, the originators of FIDNet were determined to affect those systems they could conceivably control, namely Federal civilian systems.

It was anticipated that the extensive collection and analyses of data resulting from these combined efforts would, in turn, provide indications and warnings of a pending or actual large-scale cyber attack. With further refinement of network management and profiling technologies for system tasking, correlation, warnings, indicators, and categorizing of new attack signatures, a technical solution to the identification of potential cyber attacks may be formulated. This technical solution, combined with other sources of intelligence concerning potential cyber threats and vulnerabilities, would afford national policy makers the opportunity to make prudent decisions and take appropriate actions to ensure the continued operation of the country's critical infrastructures.

Unfortunately, in the nation's capital, a good initial concept does not guarantee eventual success. With the idea of FIDNet developing steadily, but still in its early, nascent phase, the PCCIP's mandate expired. The Commission sought

out support in a logical organization for this type of program, the National Security Council. The NSC responded to the idea positively and assumed control of the project. Regrettably, the NSC soon strayed from the concept of a limited detection system for the federal government and began to have internal discussions of the possibility of a national intrusion detection system. It was at this stage in the Cyber Early Warning project that the whole of the venture began to unravel.

3.1.2 FIDNet Unraveled

The Federal Intrusion Detection Network (FIDNet) originally surfaced during the summer of 1999 with the disclosure of a draft of the National Plan.[15] Congress and the public became aware of FIDNet not as a result of a formal presentation but as a result of a careless and untimely disclosure by a government official, which led to a front-page story in the New York Times.[16] This was not the best way to make national policy on such an important issue. Several key stakeholders, namely Congress, public interest organizations and private industry were not briefed on the details of the proposal prior to its being made public. FIDNet generated substantial objections from civil liberties advocates and Members of Congress, as well as cynicism from information and network security specialists.

There is one primary reason for the incredible heat that was brought upon the federal government once the concept of FIDNet was leaked to the public. Principally, the FIDNet program existed largely in a nascent form. Several key programmatic decisions had not been made or even considered at this point. For example, the originators did not have any idea where the centralized intrusion detection system would reside. When reporters, privacy organizations and Congress jumped to the conclusion that a system with this capability would naturally be housed in the FBI, the NSC had no ability to confirm or deny these allegations.[17] This only fueled the speculation by critics and privacy advocates that the federal government was attempting to broaden its “Big Brother” surveillance and monitoring capability into the cyber world.[18] All of the tough questions any program must face in its early stages of development were brought upon the NSC in a highly visible arena.

From the time of FIDNet’s first public exposure, the program evolved and changed consistent with rising and lowering levels of interest and influence of certain organizations both within the federal government and outside as well. The White House had low interest in FIDNet throughout its development. This is clear evidence that the project never moved beyond a minor issue in the Clinton Administration’s elite policy community. The NSC initially began with a significant level of interest. However, as the project became more burdensome, the NSC became less vocal, pushing the matter off its table of issues. External factors also made the NSC less interested in FIDNet. For example, Y2K preparations were in full swing as the news of FIDNet became public. Dedicating

analytical time to a still undeveloped, highly visible technical program was not something the NSC was willing to pursue at the time.

Once the program became public, numerous key players performed a "Washingtonesque" dance to position themselves correctly for the ensuing battle. Because the NSC, FBI, etc. had not defined the program adequately, the U.S. Congress and privacy advocates from all over leapt to the spotlight to ensure their voices were heard. In Congress, Senator Kyl, Feinstein, and Biden, held hearings to discuss the potential privacy and civil liberty violations inherent in the proposed centralized monitoring system.[19] The Senators requested numerous reports and responses to Questions for the Record be reported to them by the CIAO. The Director of the CIAO, John Tritak, was asked to testify numerous times[20] as was "privacy expert" Mark Rotenberg, Executive Director of the Electronic Privacy Information Center (EPIC).

Mr. Rotenberg represents a segment of Washington that relies on funding from Congressional representatives to support their various causes. Therefore, if Capital Hill is interested in an issue, so is Mr. Rotenberg's organization. This dynamic is evidenced quite vividly in EPIC's quick strike, public outcry over FIDNet.[21] Naturally, EPIC inadvisably relied on bits of information gained from various sources and pieced together an onslaught on FIDNet full of inaccuracies and overstatements. Although much of what EPIC reported was inaccurate, such as their claim that the FBI was going to use private credit card records and telephone toll records as part of the intrusion detection system, the barrage was successful.[22] What Mr. Rotenberg failed to understand was that FIDNet was an examination of the underlying technology only, and had nothing to do with using actual phone number or credit card records.[23]

Due to the increased pressure and scrutiny being levied on the NSC and FBI, both agencies decided the program was not worth salvaging, at least by their respective organizations. The realization came quickly that mistakes had been made early on, primarily in not defining the program clearly before publicly releasing (intentionally or unintentionally) a not well thought out concept. Rather than fight the uphill battle, the agencies lost interest in the concept altogether, instead preferring to take up the concept at a later date.

3.2 Current National Plan

The FIDNet envisioned in the first National Plan would have been a government-wide system using artificial intelligence intrusion detection software to monitor contacts with sensitive government computers in an effort to identify suspicious behavior. Intrusion detection monitors installed on individual systems or networks would be "netted" or linked to a central analysis unit so that patterns across systems could be identified and all sites could be warned of intruders or intrusion techniques used at one site. As first proposed, the central analysis unit was the Federal Bureau of Investigation's National Infrastructure Protection Center (NIPC). In the final Plan, it is at the General Service Administration's Federal Computer Incident Response Capability (FedCIRC). The draft plan

indicated that FIDNet eventually would be extended to private sector systems as well, but that concept did not appear in the final plan.[24]

The February 2003 release of the new National Strategy to Secure Cyberspace departs dramatically from the original National Plan's vision of a cyber early warning system.[25] It appears as though the new author's carefully studied the lessons learned from the previous FIDNet debacle and created a more palatable, although not necessarily useful, solution. For example, the authorizing legislation for the Department of Homeland Security (DHS) created a privacy officer position to "ensure that any mechanisms associated with the National Cyberspace Security Response System appropriately balance its mission with civil liberty and privacy concerns."[26]

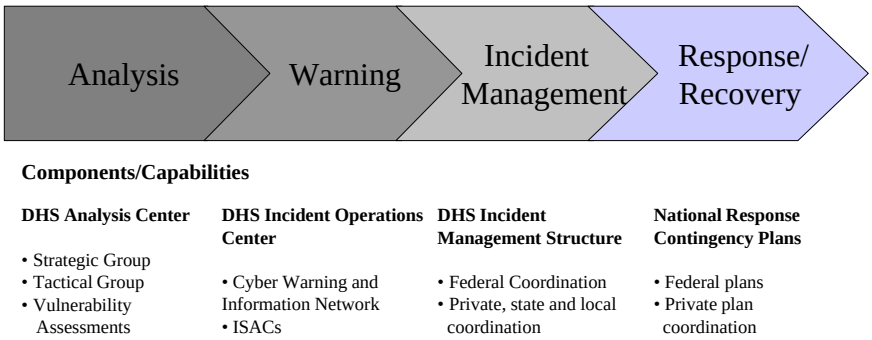
Previous attempts at Critical Infrastructure Protection were scattered across the federal government with loose organization provided by the Critical Infrastructure Assurance Office (CIAO). The new plan integrates the majority of the CIP functions into the recently created DHS. This consolidation should greatly improve information sharing not only among the federal government, but with the private sector as well.

DHS is tagged to develop the National Cyberspace Security Response System, a Priority 1 initiative in the new National Plan. The National Cyberspace Security Response System is designed to be a public-private architecture for:

- Analysis and warning;
- Managing incidents of national significance;
- Promoting continuity in government systems and private sector infrastructures; and,
- Increasing information sharing across and between organizations to improve cyberspace security.[27]

The graphic below demonstrates the architecture designed to manage the massive amounts of data, incidents, and recovery needs of the National Information Infrastructure.

National Cyberspace Security Response System



28

The concept of FIDNet is hardly recognizable in the new National Plan. Rather than focusing on a network of sensors across the federal government to provide early warning of an attack, the Plan relies heavily on information sharing among private industry sectors and within the federal government. The "Warning" description of the National Cyberspace Security Response System describes two key initiatives to provide the critical early warning function for the National Information Infrastructure:

- Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace, and
- Expand the Cyber Warning and Information Network (CWIN) to support DHS's role in coordinating crisis management for cyberspace[29]

The first initiative does little to solve the ongoing debate within private sector industries regarding information sharing among themselves. The Plan *encourages* the private sector to develop information sharing mechanisms, such as Information Sharing and Analysis Centers (ISACs), to disseminate threat and vulnerability information. However, without significant progress on the legal front, industries are limited in the information they can share due to liability concerns and potential market advantages. While the goal of creating a synoptic view of the health of the NII is correct, the Plan again fails to put forth a sustainable solution.

The second initiative, the CWIN, may resemble the FIDNet solution if all the details were made public. The general language of the Plan does not afford a clear understanding of its intent, but some familiar language is used. For example, the CWIN intends to provide an "out-of-band private and secure communications network for government and industry, with the purpose of sharing cyber alert and warning information."[30] The Plan states that the first phase of this initiative was implemented between the federal government cyber

watch centers, but the goal will be to incorporate other critical government and private sector partners, such as ISACs. No mention is made of any FIDNet-like centralized near real-time monitoring capability. DHS will coordinate the CWIN initiative, probably in the recently acquired FedCIRC office (formerly at GSA).

4.0 CONCLUSION

The concept of early warning in cyberspace has had a long history in the U.S. government. Many government and private sector initiatives have valiantly attempted to solve one of this country's emerging threats. Fortunately, or unfortunately depending one's political leanings, the privacy and civil liberty communities have successfully resisted the creation of a central Internet monitoring capability. Perhaps the Internet's de facto design of insecure protocols across public networks will never lend itself to the same early warning advantages enjoyed decades ago. Perhaps we should rethink our entire strategy as we did after Pearl Harbor in 1941 and the successful launch of Sputnik I in 1957.

Table of References

"Associate Retired Aviation Professionals: The Flight 800 Investigation, last updated April 5, 2003,
Access online via http://www.twa800.com/index.htm (4/8/2003)

Executive Summary of "National Plan for Information Systems Protection" January 7, 2000. Accessed online via
http://www.ciao.gov/resource/pccip/intro.pdf (3/23/2003)

"Executive Order 13010 Critical Infrastructure Protection," July 15, 1996. Accessed online via http://www.fas.org/irp/offdocs/eo13010.htm (3/12/2003)

PCCIP. "Critical Foundations: Protecting American's Infrastructures," (October 1997), accessed on-line via http://www.ciao.gov/resource/pccip/intro.pdf

"Initial comments of CDT on Draft National Plan for Information Systems Protection", July 27, 1999 Jim Dempsey accessed online via
http://www.cdt.org/security/fidnet/whitehouse/. (3/22/2003)

Siemens AG, Corporate Technology Department. "Information and Communications Fraud detection in communications networks using neural and probabilistic methods", accessed online via
http://www.cis.hut.fi/jhollmen/Publications/icassp98.pdf (3/24/2003)

Compaq Telecom FIINA 2001. "Dealing with Fraud in a converging environment." accessed online via
http://telecom.compaq.com/Posts/OverviewPDF/FrostFraudPaper.pdf,
(3/21/2003)

"Defending America's Cyberspace: National Plan for Information Systems Protection, "June 6, 1999. accessed online via
http://www.ciao.gov/resource/np1final.pdf. (3/24/2003)

Markoff, John, "U.S. Drawing Plan that will monitor computer systems." N.Y. Times. July 28, 1999.

Testimony and Statement for the Record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, Washington,, DC. Hearing on CyberAttack: The National Protection Plan and its Privacy Implications. Before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information. United States Senate. Dirksen Senate Office Building Room 226, February 1, 2000.

Senator Kyl, Senator Feinstein, and Senator Biden, Questions for the Record, Subcommittee on Technology, Terrorism and Government Information,

Committee on the Judiciary, United States Senate. February 1, 2000. Received in hard copy.

"A National Cyberspace Security Response System." Accessed online via http://www.whitehouse.gov/pcipb/priority_1.pdf (4/4/2003)

---

[1]"Associate Retired Aviation Professionals: The Flight 800 Investigation, last updated April 5, 2003, http://www.twa800.com/index.htm (4/8/2003)
[2] Executive Summary of "National Plan for Information Systems Protection" January 7, 2000. http://www.ciao.gov/resource/pccip/intro.pdf (3/23/2003)
[3] "Executive Order 13010 Critical Infrastructure Protection," July 15, 1996. http://www.fas.org/irp/offdocs/eo13010.htm (3/12/2003)
[4] E.O. 13010.
[5] E.O. 13010.
[6] PCCIP. "Critical Foundations: Protecting American's Infrastructures," (October 1997). http://www.ciao.gov/resource/pccip/intro.pdf
[7] PCCIP. No page number. See http://www.ciao.gov/resource/pccip/intro.pdf
[8] PCCIP , p. 58.
[9] PCCIP Report, supra note 2 at 58-9, 91. The concept of monitoring communications networks also was approved at the December 1997 meeting of the Justice and Interior ministers of the G8. In their final communiqué, the ministers agreed that, "To the extent practicable, information and telecommunications systems should be designed to help prevent and detect abuse, and should also facilitate the tracing of criminals and the collection of evidence." Meeting of Justice and Interior Ministers of the Eight, "Communiqué" (December 10, 1997). http://www.qlinks.net/comdocs/washcomm.htm (3/23/2003)
[10] The PDD itself is classified. A "White Paper" explaining its key elements can be found at http://www.ciao.gov/resource/paper598.html. (3/23/2003)
[11] "Initial comments of CDT on Draft National Plan for Information Systems Protection", July 27, 1999 Jim Dempsey. http://www.cdt.org/security/fidnet/whitehouse/. (3/22/2003)
[12] Siemens AG, Corporate Technology Department. "Information and Communications Fraud detection in communications networks using neural and probabilistic methods."http://www.cis.hut.fi/jhollmen/Publications/icassp98.pdf (3/24/2003)
[13] Compaq Telecom FIINA 2001. "Dealing with Fraud in a converging environment." Compaq Telecom FIINA 2001. http://telecom.compaq.com/Posts/OverviewPDF/FrostFraudPaper.pdf, p.5 (3/21/2003)
[14] PCCIP. "Critical Foundations: Protecting American's Infrastructures." (October 1997). http://www.ciao.gov/resource/pccip/intro.pdf (4/1/2003)
[15] "Defending America's Cyberspace: National Plan for Information Systems Protection, "June 6, 1999. http://www.ciao.gov/resource/np1final.pdf. (3/24/2003)

[16] Markoff, John, "U.S. Drawing Plan that will monitor computer systems." N.Y. Times. July 28, 1999. A1.
[17] Testimony and Statement for the Record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, Washington,, DC. Hearing on CyberAttack: The National Protection Plan and its Privacy Implications. Before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information. United States Senate. Dirksen Senate Office Building Room 226, February 1, 2000. p. 2.
[18] Rotenberg, Mark. Testimony. p. 25
[19] Senator Kyl, Senator Feinstein, and Senator Biden, Questions for the Record, Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, United States Senate. February 1, 2000. Received in hard copy.
[20] Statement of John S. Tritak, Director of the Critical Infrastructure Assurance Office, Hearing before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information, February 1, 2000. Received in hard copy.
[21] Electronic Privacy Information Center. "Privacy Center Challenges Government Surveillance Plan." http://www.epic.org/security/cip/press_release_0200.html (3/26/2003)
[22] Rotenberg, Marc testimony. http://www.epic.org/security/cip/press_release_0200.html.
[23] Statement of John S. Tritak, Director of the Critical Infrastructure Assurance Office, Hearing before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information, February 1, 2000. Received in hard copy.
[24] See National Plan, supra note 10 at xix-xxi, 13-14, 37-42.
[25] "A National Cyberspace Security Response System." http://www.whitehouse.gov/pcipb/priority_1.pdf (4/4/2003)
[26] "A National Cyberspace Security Response System." p.20.
[27] "A National Cyberspace Security Response System." p.20.
[28] "A National Cyberspace Security Response System." p.21.
[29] "A National Cyberspace Security Response System." p. 23.
[30] "A National Cyberspace Security Response System." p. 23.

Last Updated: July 20th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, GB	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Pen Test Berlin 2018	OnlineDE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced